Biometrica FRT Overview and Recommended Use Policy for Law Enforcement Agencies Utilizing Facial Recognition Through Biometrica's Systems

Purpose of Policy

The purpose of this policy is to provide guidance on the use of facial recognition technology (FRT) by law enforcement and to recommend guidelines, policies, procedures for its proper use and accountability. This policy will ensure that all FRT use is consistent with authorized purposes while not violating the privacy, civil rights, and civil liberties of individuals — FRT must be used in a manner consistent with the requirements and protection of the Constitution of the United States and other applicable statutory authorities.

This document outlines the best practices, compliance framework, and recommended use policy for law enforcement agencies partnering with Biometrica. It provides guidelines for responsible, ethical, and legally compliant use of FRT in law enforcement operations while ensuring adherence to a range of applicable biometric and data privacy laws, and civil liberties protections. It is also the purpose of this overview to provide Company personnel and credentialed law enforcement partners with guidelines and principles for the collection, access, use, retention, deletion and purging of images and related information applicable to the implementation of an FRT program.

Company Overview

It is to be noted that Biometrica is not a facial recognition company and therefore has no access to biometrics or biometric identifiers. It is a big data and software solutions company that provides licensed and trained users with a legally permissible purpose to have access to FRT as one of its tools, while searching against its UMbRA database or by comparative matching of submitted images through its QAPLA 1:1 image comparison tool.

Biometrica does not develop or maintain its own algorithms. It is "algorithm agnostic." The Company licenses NIST-evaluated and approved third-party facial recognition algorithms for lawful use in authorized searches against its 100% law enforcement-sourced data. These third-party algorithms operate in an isolated and secure black box environment that Biometrica staff have no access to.

What is UMbRA?

UMbRA is a searchable, multi-jurisdictional, real-time database of 100% law enforcement-sourced non-biometric data only, which includes charge or booking data, criminal data, sex offender registration data, parole/probation data, and warrant data. Additionally, UMbRA records may contain non-searchable information inputted by law enforcement, related to missing persons.

Who has access to UMbRA?

Direct UMbRA database access is restricted to law enforcement and mission-aligned partners operating in support of law enforcement. Specifically, access is limited to:

1. Credentialed and trained personnel from law enforcement agencies.
2. Credentialed and trained personnel from quasi-law enforcement entities — like DA's/AG's office investigators, fusion centers, transit police or special jurisdictional units, State Gaming Control Boards or ABC Enforcement, etc.
3. Credentialed and trained individuals from mission-aligned partners working in support of law enforcement, other government agencies, and other legitimate and authorized criminal investigations or public safety operations — including participants in Organized Retail Crime task forces, financial crimes investigations, national security and critical infrastructure protection operations, anti-human trafficking initiatives, child protection task forces, joint investigative operations, or formal public-private safety partnerships.

Note: All search queries are private to a credentialed user. Biometrica staff have no access to queried data or search results through UMbRA (or QAPLA). UMbRA may only be used in support of legitimate and authorized investigative, victim ID and recovery, national security, critical infrastructure protection, anti-financial crime, asset protection, or public safety purposes. All UMbRA users are subject to Biometrica's credentialing, training, and audit requirements, and the recommended FRT use policy for law enforcement, which also applies to analysts/investigators associated with agencies.

Please note the following:

- We do not ingest juvenile offender data into the UMbRA database, unless that minor has been charged as an adult.
- We do not sell any data to third-party advertisers.
- We do not make our records publicly available/accessible on any site/website.
- All access to law enforcement is controlled and every process has an immutable audit trail for legal purposes.

- We are compliant with current global privacy laws, including and not limited to the GDPR, the UK DPA, the European AI Act, the 2022 Quebec law and all US federal and state biometric and data privacy laws.
- UMbRA searches are private to a law enforcement agency. Biometrica staff have no access to a search done by any officer, analyst or investigator.

The UMbRA database is built entirely from law enforcement data, and we do not incorporate data from non-law enforcement sources, such as social media, property records, credit histories, drivers' licenses, or other databases. This guarantees that only individuals who are relevant to law enforcement because of a known and adjudicated event are compared. While Biometrica may format data received from law enforcement in order to standardize it, or merge records/events on the same individual into a single "file" for easier user access, we do not edit, alter, or supplement a law enforcement-sourced record or event, even if there is a possible error, like an evident spelling mistake, in order to maintain a digital chain of custody and validate data provenance.

Why did Biometrica implement an FRT program?

Facial Recognition involves the ability to examine and compare distinguishing characteristics of a human face through the use of biometric algorithms contained within a software application. The technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health, life, or public safety, locate missing persons, protect children and vulnerable adults, assist in matters of national security, and help in the identification of persons unable to identify themselves or of deceased persons.

Why The Company Needed A Customized Biometric Data Policy

According to the Department of Justice's Bureau of Justice Assistance (BJA), "There is no uniform set of rules in the United States governing the gathering, collection, use, sharing, and dissemination of information available through facial recognition tools. The potential for misuse of face recognition information may expose agencies participating in such systems to civil liability and negative public perceptions. The lack of rules and protocols also raises concerns that law enforcement agencies will use face recognition systems to systematically, and without human intervention, identify members of the public and monitor individuals' actions and movements. Strong control and oversight of face recognition use are critical considerations in policy development and program implementation. Such efforts not only enhance mission effectiveness but also safeguard the privacy, civil rights and civil liberties (P/CRCL) of individuals."

Given the Company's focus on public safety and partnerships with law enforcement, it was felt it was reasonable to develop a biometric data policy that was based on models developed by various state, local, and federal law enforcement, their privacy counsel, and criminal justice partners, to provide law enforcement partners with a permissible purpose and a framework for developing facial recognition policies that complied with applicable laws, reduced privacy risks, implemented minimum required training for authorized users and examiners, protected individuals' privacy, civil rights and civil liberties, and established Company accountability and oversight. However, it was also felt it was equally important to build upon and enhance existing model policies and provide a detailed overview of the subject matter in a clear and consistent manner.

How Do Face Recognition Systems Work?

At its very basic, Facial Recognition, which was created by the application of mathematical techniques to the study of the human brain, has four elements to its technology:

- The Algorithm, inspired by the human brain.
- The Camera, in order to have vision, inspired by the human eye.
- The Database, needed in order to have a memory of known and unknown humans, inspired by the ability of a human memory to remember faces (a typical human can recall about 5,000 faces across their lifetime).
- Processing Power, also inspired by the innate processes of the human brain.

As a biometric system, a Facial Recognition system, as generally understood, operates in either or both of two modes when a face is detected:

- Face Verification (or Authentication)
- Face Identification (or Recognition)

What is Face Authentication? Face authentication or verification involves a one-to-one match that compares a query face image against a single enrollment face image whose identity is being claimed. Verification of an individual for a self-serviced immigration clearance using an E-passport is one typical application of this. Matching your own face against your phone is another example.

What is Face Identification? Face identification or recognition involves 1:Many matching that compares a queried face against multiple faces in an enrollment database, in order to associate the identity of the queried face to one of those in the database. In some identification applications, one just needs to find the most similar face. In a background check or face identification being done for an investigatory lead, the requirement is more than finding similar faces; typically, a confidence level threshold is specified and all those faces whose similarity score is above the threshold are reported.

Note: The performance of FRT largely depends on a variety of factors such as lighting, facial pose, expression, age span, hair, facial wear, source device, modifications and motion, in addition to the diversity of the dataset and the data the algorithm was trained against.

In Biometrica's case, our third-party NIST-approved algorithms run a query via our UMbRA database in a black box environment where all biometric processing is fully isolated from Biometrica's systems. All searches remain private to the law enforcement agency conducting the search but there is an audit trail for legal and review purposes.

The algorithms in use are FedRAMP (Moderate and High) authorized. FedRAMP stands for Federal Risk and Authorization Management Program, and the algorithmic evaluation is based on the NIST Special publication 800-53.

What is a black box environment in this case?

- Biometrica does not access, transmit, retain or store any biometric templates, information or identifiers. Biometrica, therefore, does not maintain a gallery of biometric templates (faceprints). We are not a facial recognition company: An image is not a faceprint (biometric). We only process images, and we neither generate nor have access to any facial template or any information extracted from that facial template, that is, we have no biometric identifiers or biometric information.
- As there is also no access to a faceprint at our end at any point of the process, there is therefore, no disposal of any faceprint required at any point by us.
- The biometric template that is generated when a facial recognition scan is run by the third-party algorithm is not available to Biometrica and is deleted and purged from the server by the algorithm on the completion of every search query sent by UMbRA.
- Within UMbRA, the images live in a separate database at the backend, separate from any associated demographic information, that is, names, charges, etc., associated with that image are each in a separate dataset. The third-party algorithm has no access to any law enforcement demographic or other data associated with an image; they only have access to the image itself and return a record number associated with that image. This provides an additional layer for data protection and data privacy.

Permitted Law Enforcement Uses of FRT, Using Biometrica's Systems

Authorized uses of FRT are limited to the following for law enforcement partners using any of Biometrica's tools:

- To identify an individual when there is a reasonable and legally justifiable basis to believe that such individual has committed, is committing, or is about to commit a crime. Agencies must follow applicable jurisdictional law for the use of FRT in their jurisdiction, based on the type of crime. For example, most jurisdictions permit the

use of FRT by trained personnel for investigations under the following circumstances or crimes (this is not a definitive list): Human trafficking, other crimes involving trafficking, including the trafficking of drugs like fentanyl, child sexual abuse material (child pornography), first or second degree child abuse, a firearm or weapons crime, crimes of violence, including sexual violence, a hate crime as defined by applicable law, a fugitive from justice, stalking and harassment, aggravated cruelty to animals,

- To identify an individual when there is a basis to believe that such individual is a missing person, victim of a crime, or witness to criminal activity.
- For any other explicit purpose that is legally permissible under the laws of the applicable jurisdiction.
- To identify a deceased person.
- To identify a person who is incapacitated or otherwise unable to identify themselves.
- To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification.
- To mitigate an imminent threat to public health, national security or public safety (e.g., to thwart an active terrorism scheme or plot), or to life and limb.
- For criminal analyses and investigations, where a potential FRT match could serve as a lead for additional steps.
- For forensic review and auditing purposes.

Prohibited Uses While Using FRT Via Biometrica's Systems

FRT must **not** be used for the following (this is not a definitive list and needs to take into account all applicable laws for a jurisdiction):

- Mass surveillance or indiscriminate tracking of individuals.
- Automated real-time identification done solely via live image or video feeds.
- Targeting individuals based on gender, race, religion, nationality, ethnicity, sexual orientation, disability, political beliefs, unhoused status, or any other protected characteristics under applicable law.
- Monitoring lawful First Amendment-protected activities.
- As the sole basis for arrest, prosecution, or obtaining a search warrant.
- Analyzing a manually produced or AI generated image or sketch.

Basic Guidance Relating To The Use of FR Against Data In UMbRA

- Facial Recognition Technology must only be used for a legitimate purpose.
- It cannot and must not be the sole criteria used for any decision, pre-adverse or adverse action, or otherwise. It is to be considered only in the light of pointer data (data that points you in a certain direction) or as an informational lead.

- It cannot and must not be the sole criteria to establish probable cause or the positive identification of an individual in a criminal investigation or proceeding.
- It does not establish probable cause to arrest or obtain a search or other warrant and is intended as a lead for additional investigative steps. Probable cause or a positive ID using FRT must be supported by additional, independently sourced evidence establishing the same.
- FRT should not be used on a sketch or an artist or AI rendering of a face.
- Any algorithmic recommendations require to be analyzed by more than one trained human analyst/reviewer prior to establishing a possible match candidate. An investigator assigned to that case must establish, with other corroborating evidence, that the suspect identified by a match is the perpetrator in the alleged crime.
- Any determination of a match made through FRT should always be based on a combination of algorithmically generated comparisons and trained human analysis.
- That trained human analysis should optimally include a review of the images used in the determination of a match to determine suitability for use, and then a review of the determination of the match itself by a supervisor certified to oversee an FRT program, or a trained colleague of the decision-maker.
- Biometrica would strongly recommend that a review process is created, implemented, codified and audited periodically by any organization using FRT, based on applicable laws of the jurisdiction/s the the law enforcement agency is governed by. This includes designating a person at the agency that is responsible for overseeing the administration of FRT use for that agency and maintaining the results of any audit for the period prescribed by law. If there is no jurisdictionally prescribed period, Biometrica would recommend maintaining records for at least 3 years post an audit.
- Facial recognition works best as a combination of human and machine intelligence: The algorithm does the first part of sifting through reams of data in seconds and filtering out the noise to provide a possible match or matches with a confidence rating, but the human, not the algorithm is always and should always be the final decision-maker. This is essential and should be non-negotiable for any agency.

Recommended Guidance On Images Submitted For FR Queries

- Biometrica strongly recommends that any submitted probe or trigger image that is modified or altered prior to submission for a FR query, should have the process of that modification or alteration documented and signed off on by a supervisor certified to oversee an FRT program.
- Any image alteration or modification may cause a misidentification and/or legal/prosecutorial questions at a later stage, in addition to potentially causing misidentification.

- If a modified or altered image requires to be used, Biometrica strongly recommends that both the original image and the modified or altered image are retained separately, along with edit logs (for example, in Adobe Photoshop), and any output from the modified image that is provided to an investigator.
- For elaboration, alterations or modifications to a probe or trigger image include the following: Cropping, resizing, rotating of an image, blurring of backgrounds, straightening, correcting a facial pose, color/tint correction, de-blurring or sharpening, lens distortion correction, dewarping, red-eye reduction, changing colors, changing hair, adding or removing head coverings, adding or removing face coverings, adding or removing facial marks, adding or removing makeup, adding or removing eyeglasses, adding or removing filters, using AI-generated images.
- Images with eyes and/or faces obscured by sunglasses should not be submitted.
- Except in exceptional circumstances, Biometrica strongly recommends that images from fisheye cameras and wide-angle lenses are not used, because face recognition often suffers from a performance degradation in accuracy when applied to images captured by fisheye cameras or wide-angle lenses, as they use a process that causes a distortion in facial features. Fisheye cameras and wide-angle lenses, for example, are best suited for providing situational or environmental awareness for users monitoring a wide area instead of applications like facial recognition.
- As a matter of policy, Biometrica recommends that any original image and the altered or modified image should both be run against UMbRA and QAPLA (the latter for verification) and records should be kept of query search results, including and not limited to any that produce a different candidate set or result.

Training & Certification: Recommendations & Requirements

- Direct access to the UMbRA database is restricted only to credentialed users within authorized law enforcement, quasi-law enforcement agencies and mission-aligned partners working in support of law enforcement who have been trained in the use of Biometrica's tools by Biometrica trainers.
- Agencies must have internal review procedures in place to validate facial recognition matches before taking action on the basis of a matched ID.

Transparency & Audits

- All FRT searches must be logged and reviewed for compliance.
- Agencies should conduct regular audits to ensure proper usage.
- All access is strictly role-based and encrypted for security.

Customized Law Enforcement Training by Biometrica

At Biometrica, our mission is focused on supporting community policing and community stakeholders within and beyond law enforcement through real-time threat detection and victim recovery, while ensuring privacy protections and audit trails are in place. To ensure the ethical use of our data and technology, Biometrica would be willing to provide customized free annual training for law enforcement partners, based on their unique needs. The basic training module will focus on training in facial identification and preventing bias in the use of big data and facial recognition. While this will continue to evolve, along with changes to law and technology, it would cover the following essential areas:

1. **What is facial recognition**? The difference between face detection, face authentication, face verification, face identification. Known and unknown faces. What is a search algorithm?

2. **Understanding when not to use FRT** : What images make sense to use, when to use a FR algorithm, when to discard image data, how to use FRT as a supplemental investigative tool in critical investigations, and how and when not to use it at all.

3. **Preventing human bias, explicit or implicit**: Understanding bias + how to recognize faces, distinguish features and understand the differences between how algorithms read data and humans look at faces.

4. **Understanding algorithmic intelligence & HUMINT**: Algorithmic tools and human frailties + algorithmic limitations and human intelligence — making technological systems work more equitably for law enforcement and the communities they protect and serve.

5. **The need for diversity in data and in training datasets and why this matters**: What data sets to use and when. False positives, false negatives, sampling errors, and confidence ratings.

6. **Checks and balances**: How do you ensure accountability and transparency? How do you limit the scope for abuse? How do you create digital audit trails to track abuse of technological tools? What processes need to be put in place while using pointer data from FR as possible informational leads? What review processes are needed and how to implement audit protocols.

This training would assist law enforcement partners in their use of our tools in a way that fosters equity, trust, and accountability, in line with their unique community engagement goals.

Conclusion

Biometrica provides law enforcement agencies with secure, privacy-first FRT tools that align with best practices for ethical use, public safety, and civil liberties protection. By following

this recommended use policy and customizing it to their own jurisdictional and statutory laws, law enforcement agencies can responsibly leverage FRT while ensuring transparency, accountability, and privacy protections.

While the laws governing biometrics in criminal investigations vary by jurisdiction, Biometrica strongly recommends that any law enforcement agency that uses our tools, develops its own standardized FRT submission request and confirmation-by-a-trained-analyst procedures, keeping in mind applicable laws. For example, depending on a state's own requirements, officers seeking facial recognition analysis may need to complete an FRT Request Form before submitting a query to a trained investigator in their agency, also documenting the following: case number and investigation type; specific investigative purpose justifying FRT use; source and unaltered condition of probe image(s); supervising officer authorization. This is just an example.

However, do note that Biometrica will be happy to provide reporting templates and technical assistance to partner agencies to facilitate efficient and complete compliance with specific reporting requirements, transforming a compliance obligation into an opportunity for demonstrating responsible innovation in public safety technology and a community-focused partnership.

For more information, please contact:

Biometrica Systems, Inc.

leo@biometrica.com (For law enforcement-related queries)

privacy@biometrica.com (For clarity on privacy, data management or biometric policies)

Version: April 2025